New Jersey Law Journal

VOL. CXCIIV - NO.10 - INDEX 826 DECEMBER 8, 2008 ESTABLISHED 1878

Employment & Immigration Law

The Impact of the Digital Age

Technology is affecting how lawyers represent their clients

By Michael N. Morea and Michael R. Yellin

Technology pervades everyone's daily life. Sometimes technology makes life simpler and at times it makes life more complicated, but as lawyers, our involvement with technology goes beyond simply our use of it. All lawyers, and employment lawyers in particular, need to be aware of how technology can affect their practices and how to advise their clients to use, or in some cases not use, certain technologies in order to best protect clients' interests. This article will examine three areas where technology has impacted employment law and practice: e-mail communications with clients, claims asserted under the Computer Fraud and Abuse Act, and employer liability for accidents caused by an employee driving while using a cell phone.

Attorney-Client Privilege in E-mails

How many lawyers have clients that communicate with them from e-mails sent from the client's office e-mail address? Presumably all lawyers' e-mails contain the ubiquitous disclaimer at the bottom of their e-mails announcing the confidential nature of the e-mail, but is that enough to protect the attorney-client privilege when the client is communicating from work? The answer is not the simple "yes" that most attorneys and clients would presume. Although there is a scarcity of published decisions on the issue of the confidentiality of e-mails sent from or received at work, courts that have decided the issue have uniformly applied the "reasonable expectation of privacy" test used in Fourth Amendment cases. In other words, the attorney-client privilege will only attach to such e-mails if the client had a reasonable expectation of the privacy in the use of the employer's computer systems.

In the context of workplace e-mail communications with counsel, a court will consider the following factors to determine if a privilege has been waived:

> (1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or e-mail, (3) do third parties have a right of access to the computer or e-mails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?
>
> *In re Asia Global Crossing, Ltd.*, 322 B.R. 247, 257 (S.D.N.Y. 2005).

If the answer to all of these questions is in the affirmative, no privilege will attach to the communication. This is true despite any pro forma disclaimer regarding confidentiality that may be appended to an attorney's e-mail. *Scott v. Beth Israel Medical Center, Inc.,* 847 N.Y.S.2d 436 (2007). The reasonable expectation of privacy analysis has been adopted by at least one New Jersey federal court in an unpublished decision. See *Kaufman v. Sungard Investment Systems, Inc*., 2006 WL 1307882 (D.N.J. May 10, 2006). Thus, if an employer, as many employers do, has a published policy restricting the use of its computer and e-mail systems to work related matters only and reserving the right to monitor an employee's e-mail or computer usage, the attorney-client privilege will not attach to any communications occurring through the office computer system.

Unless representing the employer, attorneys would be wise to avoid e-mail communications with clients through the e-mail system of the cli-

Morea is Special Counsel in the Employment and Litigation Departments and Yellin is an associate in the Litigation Department of Cole, Schotz, Meisel, Forman & Leonard in Hackensack.

ent's employer and should advise clients that any e-mails they send through the employer's system may not be privileged. This is especially important when representing an employee who has or may have claims against a current employer.

Computer Fraud and Abuse Act

As part of their e-mail and computer policy, employers should explicitly define to what extent employees are authorized to access information contained on the employer's computer systems. Lawyers for both employers and employees alike must be cognizant that exceeding authorized access can serve as the basis for a cause of action under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, et seq.

Although once relegated to the world of hacking and cyber-terrorism, the CFAA has dramatically expanded in scope and applicability over the past two decades. These changes have resulted in employers "increasingly taking advantage of CFAA's civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system." *P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC*, 428 F.3d 504, 510 (3d Cir. 2005) (internal citations omitted). Typically, CFAA claims arise in misappropriation of trade secret type cases.

The CFAA allows recovery for, among other things, damages for losses aggregating at least $5,000 in value during any one-year period from a person who "intentionally accesses a protected computer without authorization." 18 U.S.C. § 1030(a)(5)(A)(iii). That said, the precise boundaries of this language remain undefined.

For example, in *P.C. Yonkers*, the Third Circuit held that the employer presented a cognizable claim under the CFAA against former employees who accessed the employer's computer systems without authorization to obtain corporate data which would allow the former employees to identify where to open competing stores. Other CFAA cases have included claims against current employees who divert company information from company computer systems for their own pecuniary gain, *Dudick v. Vaccarro*, 2007 U.S. Dist. LEXIS 45953 (M.D. Pa., June 25, 2007), an employee who deleted information off a company computer without authorization, *Forge Industrial Staffing, Inc. v. De La Fuente*, WL 2982139 (N.D. Ill., Oct. 16, 2006), and an employee who allegedly diverted company trade secrets to a competitor. *PharMerica, Inc. v. Arledge,* WL 865510 (M.D. Fla., Mar. 21, 2007).

The application of the CFAA, however, has not been unbridled. In *Lockheed Martin Corp. v. Speed*, the court held that because the defendants were authorized to access both the company's computer as well as the information allegedly misappropriated, that no cause of action existed under the CFAA. 2006 WL 2683058 (M.D. Fla., Aug. 1, 2006). The court concluded that despite the breach of loyalty by the employees, Congress had clearly delineated between those "without authorization" and those "with authorization" in the statute and that the plain language of Congress would control, despite the conduct of the employee.

Where the courts will ultimately settle on the CFAA's breadth remains to be seen. To protect employers' ability to utilize the CFAA, attorneys should advise their clients to establish policies that articulate not only who is authorized to access company technology, but also the authorized scope of that access. Setting such boundaries will serve both as a sword and a shield against abuses of company technology by protecting the potential use of CFAA as a civil remedy, but also by warning employees of the consequences for exceeding the scope of their rightful access.

Accidents Caused by Cell Phone Use

As prevalent as e-mail communications and computer technology are, so are drivers using cell phones. Cell phone use while driving has become so epidemic that a number of states, including New Jersey, New York, Connecticut and the District of Columbia, have all enacted bans on the use of a hand-held cell phone or device while driving. In numerous other states hand-held bans are enacted through municipal ordinance. The extensive use of cell phones while driving has added a new wrinkle to the doctrine of respondeat superior that could, in the absence of an appropriate employer policy, cause employers to be liable for automobile accidents caused by employees.

Employers will typically only be liable for accidents caused by employees while they are working or "on the clock." Cell phone use presents a potentially unique situation where an employee might be on his or her own time, but making a business-related phone call or using an employer issued device. Generally, while on his or her own time or even when commuting to or from work, an employee is not considered to be acting within the scope of employment and liability will not attach to the employer for the employee's negligence while driving. However, when work-related cell phone use or an employer-issued handheld device is added into the picture, courts have held that the employee could be found to be acting within the scope of employment sufficient to trigger respondeat superior liability for the employer. See e.g., *Ellender v. Neff Rental, Inc.,* 965 So.2d 898 (La. App. 1 Cir. 2007); *Miller v. American Greetings Corporation,* 161 Cal. App.4th 1055 (2008).

While these and similar cases do not change the theory of respondeat superior liability, they do provide

a relatively new circumstance in which the doctrine could be triggered. Laws prohibiting the use of hand held devices while driving may provide additional grounds to hold employers liable or buttress claims of negligence to per se negligence due to the violation of a law. In order to protect employers, attorneys should advise their clients to implement a written policy prohibiting the use of hand-held devices, such as cell phones, for business purposes while driving. If the hand-held device is employer issued, the policy should provide that the use of the device while driving is prohibited regardless of whether the phone use is personal or business-related. Employers should be further advised that it is not enough to merely put the policy in writing and that the policy must be enforced. Finally, employers should be advised to have employees sign an acknowledgment of the policy before issuing hand-held devices to an employee.

As technology advances and becomes more prevalent in the day-to-day operations of businesses, it becomes increasingly crucial for employers to implement policies governing the use of technology. Policies such as the ones discussed herein can help to not only protect employer's computer and electronic information, but also serve to minimize the employers' potential liability arising from an employee's use of technology. Similarly, lawyers for both employees and management need to be aware of the employer's policies in a given matter so as to best advise and represent the respective interests of their clients. ■